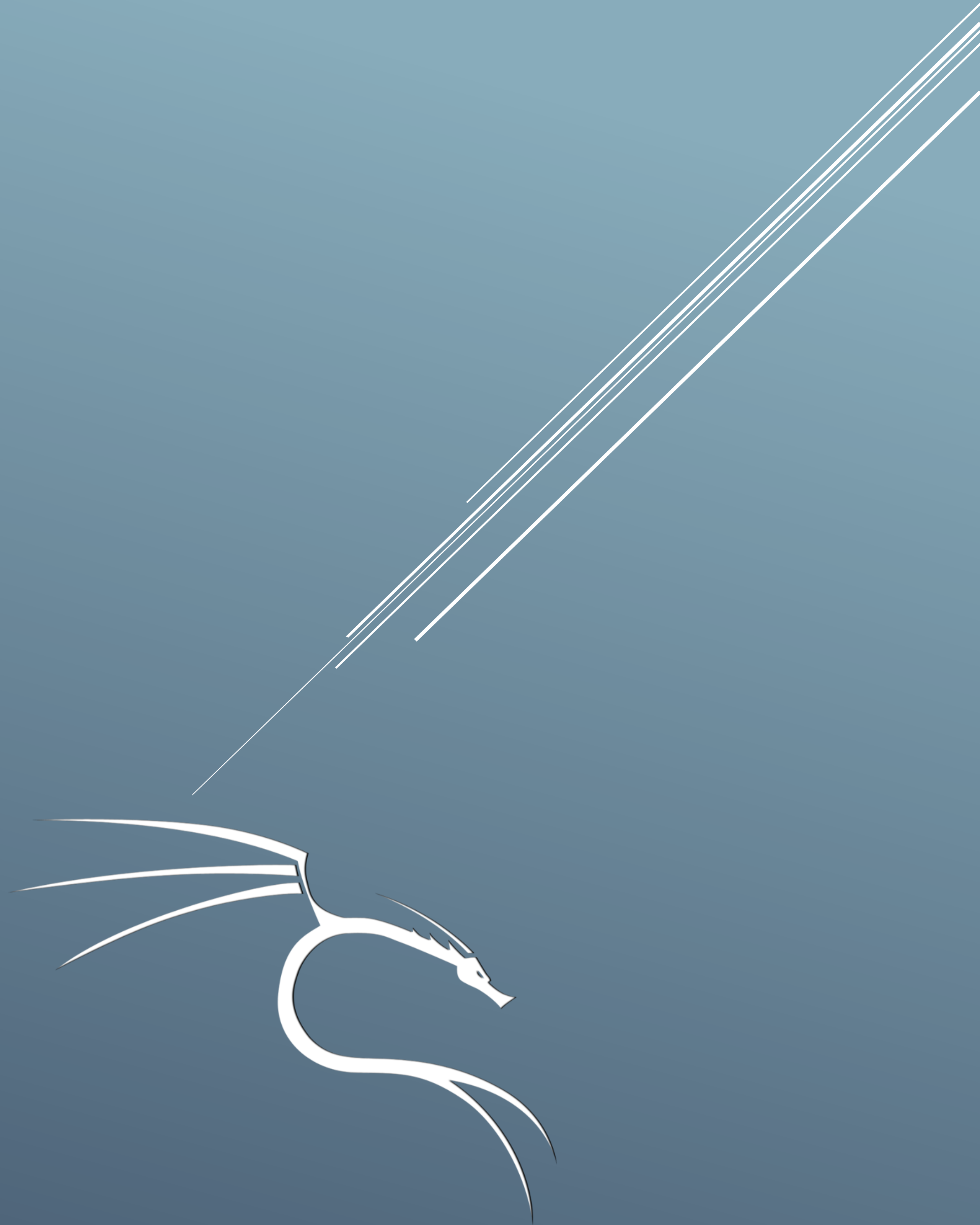


Penetration Testing with Kali Linux - Part1 (Tools)

Sirvan allahvisi – March , 2017

Author : Sirvan allahvisi

More Papers : https://independent.academia.edu/SirvanVisi

E-mail : SirvanVisi@yahoo.com

Twitter : @Sirvanvisi

25 March 2017

Kurdistan , Sanandaj

25 March - "don't forget turn off their lights for Earth Hour at 8.30pm (20:30)"

to respect our planet Earth!

مقدمه:

این روزها بخش عظیمی از اسناد و اطلاعات شرکت ها و ارگان های مهم ، سیستمی شده و روی شبکه قراردارد.حال اگر برای یک لحظه شبکه مورد نفود و حمله هکرها قرار گیرد، تمامی اسناد و اعتبارات و موارد محرمانه، مورد نفوذ قرار گرفته و مشکل ساز می شود. بنابرین نیاز داریم تا هر از گاهی میزان نفود پذیری شبکه و هر آنچه مربوط به آن است، از قبیل تمام سیستم ، نرم افزارها و سرویس های نصب شده روی آن را برای یافتن مشکلات امنیتی بررسی کنیم.

تست نفوذ یک فرآیند سیستماتیک و برنامه ریزی شده است که آسیب پذیری ها و حفره های امنیتی سرور، شبکه ، منابع و برنامه های متصل به آن را از طریق شبیه سازی یک حمله هکر، چک می کند. به صورتی که تست نفوذ می تواند با استفاده از منابع داخلی مثل سیستم امنیتی میزبان ویا منابع خارجی، کنترل و سازماندهی شود.بنابراین از این تست که یک حمله شبیه سازی شده است، برای یافتن مشکلات و سنجش میزان امنیت سرور و شبکه های متصل به آن استفاده می شود.

دراین مقاله مباحث مربوط به سیستم عامل کالی لینوکس ، ابزراها و بخش های مرتبط با آنالیز ، تست نفوذ پذیری و امنیت سرورها توضیح داده خواهد شد.
همچنین سعی بنده بر این است که کالی لینوکس و اصطلاحات مربوط به تست نفوذ را به زبان ساده تری بیان کنم تا کاربران مبتدی و علاقه مند به این موضوع نیز بتوانند از این مطالب استفاده نمایند.

Network:

برای اینکه بفهمیم چه پورت هایی روی سیستم هدف باز است ، چه سیستم هایی توی شبکه live هستن ، سیستم عامل شبکه چیه و اطلاعات تکمیلی در رابطه با اون سیستم رو بدست بیارید از ابزار nmap استفاده می کنیم.

دراین قسمت من nmap رو برای شبکه داخلی استفاده می کنم در قسمت بعدی nmap رو در سطح اینترنت آموزش خواهم داد.

برای استفاده از ابزار nmap ابتدا terminal رو باز میکنیم و دستور زیر را وارد میکنیم :

```
nmap –sn ip
```

با استفاده از این دستور میخواهیم رنج ip شبکه رو اسکن کنیم ، به جای ip عدد موردنظر خودرا وارد میکنیم ، مثلا :

```
nmap –sn 10.0.0.0/24
```

با استفاده از دستور بالا یه اسکن انجام میدیم تا ببینیم چه ip هایی داخل شبکه ما live هستند (از این دستور برای cheek for live system استفاده میکنیم).

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sn 10.0.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-07 22:06 EST
Nmap scan report for 10.0.0.10
Host is up (0.00030s latency).
MAC Address: 00:0C:29:B5:FA:B7 (VMware)
Nmap scan report for 10.0.0.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 28.26 seconds
root@kali:~#
```

طبق تصویر یک IP (۱۰,۰,۰,۱۰) دارم که در پایین مک آدرسش رو نشان داده و یک IP (۱۰,۰,۰,۱) هم هستش که برای سیستم خودم هستش.

درمرحله بعدی برای اینکه سیستم عامل هدف رو شناسایی کنیم از سوئیچ زیر استفاده میکنیم:

nmap –O 10.0.0.10

این سوئیچ سیستم عامل طرف مقابل رو به ما نشان میدهد.

```
root@kali: ~
File Edit View Search Terminal Help
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:B5:FA:B7 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wind
ows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, o
r Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.59 seconds
root@kali:~#
```

میبینید که هم سیستم عامل رو به ما نشان داد هم به ما میگه که چه پورت هایی برروی سیستم هدف باز هستش.

دستور بعدی : ما میتونیم یک پورت خاص رو مدنظر قرار بدیم مثلا پورت ۲۳ بنابراین دستور زیر را وارد میکنیم:

nmap –p 23 10.0.0.10

```
root@kali: ~
File Edit View Search Terminal Help
MAC Address: 00:0C:29:B5:FA:B7 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:wind
ows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, o
r Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.59 seconds
root@kali:~# nmap -p 23 10.0.0.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-07 22:09 EST
Nmap scan report for 10.0.0.10
Host is up (0.00047s latency).
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:29:B5:FA:B7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@kali:~#
```

طبق تصویر بالا همینجا اطلاعات رو بهمون میده و میگه پورت ۲۳ باز هست و مربوط به سرویس telnet هستش ، درپایین هم مک آدرس رو به ما نشون میده و با توجه به آدرس مک متوجه شده که این سیستم از نوع vmware است (در این آموزش من ویندوز ۷ و کالی لینوکس رو برروی vmware نصب کرده ام)

با استفاده از این دستور ما میتونیم اطلاعات تکمیلی تری رو بدست بیاریم و به اینصورت دستور رو وارد میکنیم:

nmap –sV –p 23 10.0.0.10

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 23 10.0.0.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-07 22:09 EST
Nmap scan report for 10.0.0.10
Host is up (0.00047s latency).
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:29:B5:FA:B7 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@kali:~# nmap -sV -p 23 10.0.0.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-07 22:09 EST
Nmap scan report for 10.0.0.10
Host is up (0.00041s latency).
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Microsoft Windows XP telnetd
MAC Address: 00:0C:29:B5:FA:B7 (VMware)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.49 seconds
root@kali:~#
```

طبق تصویر اطلاعات تکمیل در رابطه با اون سرویس رو به ما نشان میده ، دراینجا گفته این سرویس مربوط میشه به Windows XP ولی خب در اینجا OS من Windows 7 هستش که با استفاده از سوئیچ O– تونستم این رو استخراج بکنم.در کل اینجا اطلاعات تکمیلی تری در رابطه با اون سرویس بهتون میده.

مثلا اگر پورت ۸۰ باز باشه ، پورت ۸۰ اطلاعات مربوط به : اگر apache باشه، اگر ios باشه نسخه ، ورژن و مشخصات دیگر رو میتوانید ازش بگیرید.

Server:

دراین بخش سعی داریم تا تخصصی تر به مبحث nmap بپردازیم ، در بخش قبل به بحث network اشاره کردیم اینجا میخوام که با اسکریپت ها آشنا بشین و دستوراتی که میتوانید برای جمع آوری اطلاعات در وب سایت ها ازشون استفاده کنید.

ابتدا terminal رو باز میکنیم و دستور زیر را وارد میکنیم:

nmap –p 80 baseiran.com

دراینجا من میخام nmap رو با پورت ۸۰ سایت baseiran.com تست کنم

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 80 baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:06 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up (0.0034s latency).
rDNS record for 185.55.227.88: hosted-by.serverpars.net
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~#
```

دراینجا به ما میگه که پورت ۸۰ باز هستش و میتونم از این پورت استفاده کنم ولی خب اینترنت روش هست و سایت هم بالاهستش و داره ارائه خدمات میده.

برای دیدن یه نمونه از پورت بسته هم مثلا بجای ۸۰ من پورت ۲۳ رو میزنم:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -p 80 baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:06 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up (0.0034s latency).
rDNS record for 185.55.227.88: hosted-by.serverpars.net
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~# nmap -p 23 baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:17 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up (0.00046s latency).
rDNS record for 185.55.227.88: hosted-by.serverpars.net
PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
root@kali:~#
```

باتوجه به تصویر بالا پورت ۲۳ فیلتره یا بسته است و نمیتونه باهاش ارتباط برقرار کنه.

در ادامه اگر ما بخواهیم که اطلاعات بیشتری راجع به http بدست بیاریم ، در ابتدای دستور یک سوئیچی هست به اسم sV- اضافه میکنیم که به ما اطلاعات بیشتری در رابطه با اون سرویس میده

nmap –Sv –p 80 baseiran.com

```
root@kali: ~
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~# nmap -p 23 baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:17 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up (0.00046s latency).
rDNS record for 185.55.227.88: hosted-by.serverpars.net
PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
root@kali:~# nmap -sV -p 80 baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:24 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up (0.0039s latency).
rDNS record for 185.55.227.88: hosted-by.serverpars.net
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.95 seconds
root@kali:~#
```

همانطور که مشاهده میکنید اینجا اطلاعات کاملی به ما میده ، مثلا میگه وب سرور وب سایت موردنظر Apache است.

دستورات بعدی که میتونیم استفاده کنیم، مربوط به اسکریپت ها هستند.

اسکریپت های nmap داخل مسیر /usr/share/nmap/scripts قرار دارند برای مشاهده آنها از دستور زیر استفاده میکنیم :

1. cd /usr/share/nmap/scripts/
2. ls

```
root@kali: /usr/share/nmap/scripts
File  Edit  View  Search  Terminal  Help
root@kali:~# cd /usr/share/nmap/scripts/
root@kali:/usr/share/nmap/scripts# ls
acarsd-info.nse                         imap-capabilities.nse
address-info.nse                        imap-ntlm-info.nse
afp-brute.nse                           informix-brute.nse
afp-ls.nse                              informix-query.nse
afp-path-vuln.nse                       informix-tables.nse
afp-serverinfo.nse                      ip-forwarding.nse
afp-showmount.nse                       ip-geolocation-geobytes.nse
ajp-auth.nse                            ip-geolocation-geoplugin.nse
ajp-brute.nse                           ip-geolocation-ipinfodb.nse
ajp-headers.nse                         ip-geolocation-maxmind.nse
ajp-methods.nse                         ip-https-discover.nse
ajp-request.nse                         ipidseq.nse
allseeingeye-info.nse                   ipv6-multicast-mld-list.nse
amqp-info.nse                           ipv6-node-info.nse
asn-query.nse                           ipv6-ra-flood.nse
auth-owners.nse                         irc-botnet-channels.nse
auth-spoof.nse                          irc-brute.nse
backorifice-brute.nse                   irc-info.nse
backorifice-info.nse                    irc-sasl-brute.nse
bacnet-info.nse                         irc-unrealircd-backdoor.nse
banner.nse                              iscsi-brute.nse
bitcoin-getaddr.nse                     iscsi-info.nse
bitcoin-info.nse                        isns-info.nse
bitcoinrpc-info.nse                     jdwp-exec.nse
bittorrent-discovery.nse                jdwp-info.nse
bjnp-discover.nse                       jdwp-inject.nse
broadcast-ataoe-discover.nse            jdwp-version.nse
```

این اسکریپت ها فایل هایی هستند که با پسوند nse ذخیره میشوند که مخفف (nmap script engine) است.

شما میتوانید با استفاده از این اسکریپت ها کارهای زیادی بکنید مثلا اطلاعات مربوط به یک دامنه ، http و اطلاعات مختلف دیگری را از وب سایت موردنظر بدست بیارید.

برای استفاده از اسکریپت های nmap بسته به نیاز خود یکی از اسکریپت ها رو اجرا میکنیم ، مثلا:

```
nmap --script whois-domain baseiran.com
```

```
root@kali: /usr/share/nmap/scripts
File Edit View Search Terminal Help
Host script results:
| whois-domain:
|
| Domain name record found at whois.yoursrs.com
| Domain Name: baseiran.com
| Registry Domain ID: 2040071030_DOMAIN_COM-VRSN
| Registrar WHOIS Server: whois.yoursrs.com
| Registrar URL: http://www.realtimeregister.com
| Updated Date: 2017-03-15T19:55:42Z
| Creation Date: 2016-07-05T08:51:15Z
| Registrar Registration Expiration Date: 2017-07-05T08:51:15Z
| Registrar: REALTIME REGISTER B.V.
| Registrar IANA ID: 839
| Reseller: Base iran Co
| Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhib
ited
| Domain Status: ok http://www.icann.org/epp#ok
| Registry Registrant ID: Not Available From Registry
| Registrant Name: baseiran
| Registrant Organization: Base iran Co
| Registrant Street: Azadi sq , Base iran Co
| Registrant City: Sanandaj
| Registrant State/Province: Kurdistan
| Registrant Postal Code: 6613713951
| Registrant Country: IR
| Registrant Phone: +98.8700000000
| Registrant Phone Ext:
| Registrant Fax:
```

طبق تصویر بالا هویز سرور رو به ما نشان میده و اطلاعاتی ازقبیل مالک و ثبت کننده دامنه ، شرکت ثبت کننده ، نیم سرورها ، مشخصات تماس مالک دامنه و... را برای ما نمایش میدهد.

نکته:

در دستور بالا علاوه بر نمایش مشخصات هویز ، پورت اسکن هم انجام میشود که هم باعث افزایش زمان نمایش اطلاعات می شود و هم باعث detect شدن توسط فایروال ها می شود.برای اینکه اسکن پورت ها انجام نشود باید یکسری از سوئیچ هارو به دستور اضافه کنیم.

برای اینکار سوئیچ های Pn- و sn- که در واقع دستور No Ping هستش و Host Discovery میکنه را به دستور اضافه میکنیم:

nmap -Pn -sn --script whois-domain baseiran.com

```
root@kali: /usr/share/nmap/scripts
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/nmap/scripts# nmap -Pn -sn --script whois-domain baseiran.com

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-03-24 12:57 UTC
Nmap scan report for baseiran.com (185.55.227.88)
Host is up.
rDNS record for 185.55.227.88: hosted-by.serverpars.net

Host script results:
| whois-domain:
|
| Domain name record found at whois.yoursrs.com
| Domain Name: baseiran.com
| Registry Domain ID: 2040071030_DOMAIN_COM-VRSN
| Registrar WHOIS Server: whois.yoursrs.com
| Registrar URL: http://www.realtimeregister.com
| Updated Date: 2017-03-15T19:55:42Z
| Creation Date: 2016-07-05T08:51:15Z
| Registrar Registration Expiration Date: 2017-07-05T08:51:15Z
| Registrar: REALTIME REGISTER B.V.
| Registrar IANA ID: 839
| Reseller: Base iran Co
| Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhib
ited
| Domain Status: ok http://www.icann.org/epp#ok
| Registry Registrant ID: Not Available From Registry
| Registrant Name: baseiran
| Registrant Organization: Base iran Co
| Registrant Street: Azadi sq , Base iran Co
| Registrant City: Sanandaj
```

همانطور که میبینید فقط اطلاعات هویز را به ما نشان داده و دیگر پورت اسکن را انجام نداده است.

در این بخش نحوه جمع آوری اطلاعات از DNS رو برای شما توضیح خواهم داد.

اولین دستوری که دراینجا کاربر دارد دستور whois می باشد که اطلاعات کاملی در رابطه با اون سیستم را به ما میدهد:

whois baseiran.com

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# whois baseiran.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: BASEIRAN.COM
   Registrar: REALTIME REGISTER BV
   Sponsoring Registrar IANA ID: 839
   Whois Server: whois.yoursrs.com
   Referral URL: http://www.realtimeregister.com
   Name Server: IRNS55.SERVERPARS.COM
   Name Server: IRNS56.SERVERPARS.COM
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Updated Date: 15-mar-2017
   Creation Date: 05-jul-2016
   Expiration Date: 05-jul-2017

>>> Last update of whois database: Fri, 24 Mar 2017 08:56:37 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
```

دستور بعدی dnsenum است که با استفاده از آن میتوانید رکوردهای DNS رو استخراج کنید و از آنها برای حملات بعدی استفاده نمایید.

این مواردی که ما اینجا بدست می آوریم در حملات بعدی برای ما خیلی مفید میتونه باشه و باید از آنها استفاده کنیم:

dnsenum baseiran.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# dnsenum baseiran.com
dnsenum.pl VERSION:1.2.3

-----   baseiran.com   -----

Host's addresses:
__________________

baseiran.com.                            13005    IN    A        185.55.227.88

Name Servers:
______________

irns55.serverpars.com.                   111252   IN    A        185.55.227.86
irns56.serverpars.com.                   111252   IN    A        185.55.227.87

Mail (MX) Servers:
___________________

baseiran.com.                            13005    IN    A        185.55.227.88

Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for baseiran.com on irns55.serverpars.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for baseiran.com on irns56.serverpars.com ...
AXFR record query failed: REFUSED

brute force file not specified, bay.
root@kali:~#
```

همانطور که متوجه شدید نیم سرورها رو به ما نشان داد و ما تونستیم بفهمیم وب سایت موردنظر از کدوم شرکت میزبانی هاست گرفته ، رکورد ip هارو به ما نشان میده و اگر zone transfer هم داشته باشه بصورت لیست نشان داده می شود.بحث zone transfer زمانی اتفاق می افتد که ارتباط بین zone ها دچار مشکل میشود و تنظیمات به درستی انجام نشده باشد.

اگر یک zone transfer را بخواهم خدمتتون توضیح بدم وب سایت megacorpone.com را تست میکنم که مشکل امنیتی zone transfer دارد:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
fb.mail.gandi.net.                        2037     IN    A        217.70.184.161
fb.mail.gandi.net.                        2037     IN    A        217.70.184.163
fb.mail.gandi.net.                        2037     IN    A        217.70.184.162
spool.mail.gandi.net.                     60972    IN    A        217.70.184.6

Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for megacorpone.com on ns2.megacorpone.com ...
megacorpone.com.                          259200   IN    SOA              (
megacorpone.com.                          259200   IN    MX               10
megacorpone.com.                          259200   IN    MX               20
megacorpone.com.                          259200   IN    MX               50
megacorpone.com.                          259200   IN    MX               60
megacorpone.com.                          259200   IN    NS       ns1.megacorpone.com.
megacorpone.com.                          259200   IN    NS       ns2.megacorpone.com.
megacorpone.com.                          259200   IN    NS       ns3.megacorpone.com.
admin.megacorpone.com.                    259200   IN    A        38.100.193.83
beta.megacorpone.com.                     259200   IN    A        38.100.193.69
fs1.megacorpone.com.                      259200   IN    A        38.100.193.82
intranet.megacorpone.com.                 259200   IN    A        38.100.193.81
mail.megacorpone.com.                     259200   IN    A        38.100.193.84
mail2.megacorpone.com.                    259200   IN    A        38.100.193.73
ns1.megacorpone.com.                      259200   IN    A        38.100.193.70
ns2.megacorpone.com.                      259200   IN    A        38.100.193.80
ns3.megacorpone.com.                      259200   IN    A        38.100.193.90
router.megacorpone.com.                   259200   IN    A        38.100.193.91
siem.megacorpone.com.                     259200   IN    A        38.100.193.89
snmp.megacorpone.com.                     259200   IN    A        38.100.193.85
support.megacorpone.com.                  259200   IN    A        173.246.47.170
syslog.megacorpone.com.                   259200   IN    A        38.100.193.66
test.megacorpone.com.                     259200   IN    A        38.100.193.67
vpn.megacorpone.com.                      259200   IN    A        38.100.193.77
www.megacorpone.com.                      259200   IN    A        38.100.193.76
www2.megacorpone.com.                     259200   IN    A        38.100.193.79
```

مشاهده میکنید که کل اطلاعات مربوط به دامین ها و رکوردهایی که وجود دارند برای ما نشان داده میشود.

مثلا در تصویر بالا رکورد های : A , NS , MX ، IP هاشون و اطلاعات کاملی در مورد zone اون وب سایت به ما نشان داده شده است.

دستور بعدی که میتونیم ازش استفاده کنیم دستوری است تحت عنوان ”dmitry“

dmitry -wnpb

این دستور میتونه کارهای مختلفی را انجام بدهد و سوئیچ های کاربردی مختلفی رو در اختیار ما قرار میده ، مثلا سوئیچ w- برای ما whois میگیره سوئیچ n اطلاعات سایت نت کرافت رو به ما میده که میتونیم ازش اطلاعات خیلی خوبی استخراج کنیم ، سوئیچ p پورت های tcp روی اون سرور رو نشون میده و سوئیچ b بنرها رو به ما نشان میدهد.

برای مثلا میخوام این تست رو برروی وب سایت megacorpone.com انجام بدم:

dmitry -wnpb megacorpone.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Gathered Netcraft information for megacorpone.com
---------------------------------

Retrieving Netcraft.com information for megacorpone.com
Netcraft.com Information gathered

Gathered TCP Port information for 38.100.193.76
---------------------------------

 Port           State

22/tcp          open
>> SSH-2.0-OpenSSH_6.0p1 Debian-3ubuntu1.2

80/tcp          open

Portscan Finished: Scanned 150 ports, 147 ports were in state closed


All scans completed, exiting
root@kali:~#
```

ملاحظه کردید که اطلاعات مربوط به رکوردها ، whois و پورت های tcp رو به ما نشان داد.

دستور بعدی که میتونیم ازش استفاده کنیم دستوری است تحت عنوان "fierce"

با استفاده از این دستور شما میتوانید اطلاعات مربوط به یک DNS و ساب دامین هاش رو بدست بیارید.

مثلا در اینجا از دستور dns- استفاده میکنیم:

fierce -dns baseiran.com

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# fierce -dns baseiran.com
DNS Servers for baseiran.com:
        irns55.serverpars.com
        irns56.serverpars.com

Trying zone transfer first...
        Testing irns55.serverpars.com
                Request timed out or transfer not allowed.
        Testing irns56.serverpars.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
185.55.227.88   ftp.baseiran.com
185.55.227.88   mail.baseiran.com
185.55.227.88   my.baseiran.com
185.55.227.88   whois.baseiran.com
185.55.227.88   www.baseiran.com

Subnets found (may want to probe here using nmap or unicornscan):
        185.55.227.0-255 : 5 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 5 entries.

Have a nice day.
root@kali:~# 
```

میبینید که اطلاعات مربوط به NS هاش رو بهمون نشان میده و همچنین اطلاعات ساب دامین ها و مشخصات دامین های دیگرش رو هم برای ما لیست میکنه و میتوانیم این اطلاعات رو برای مراحل بعدی داشته باشیم.

ما این اطلاعاتی که اینجا بدست می آوریم را یادداشت می کنیم تا بعدا در هنگام حملات بتونیم از آنها استفاده کنیم.

در این قسمت ۲ ابزار مهم و خیلی مفید جمع آوری اطلاعات را به شما معرفی میکنم.

اولین ابزار "theharvester" می باشد که برای جمع آوری اطلاعات مربوط به ساب دامین ها و ایمیل ها میشه ازش استفاده کرد.این ابزار از بخش های مختلفی از موتورهای جستجو گوناگون میتونه استفاده بکنه ، از google ، bing و یا اطلاعات مربوط به linkedin رو استخراج کند.

برای مثال من میخوام ایمیل هایی که داخل baseiran.com است رو استخراج کنم بنابرین دستور رو اینجوری تایپ میکنم:

theharvester -d baseiran.com -l 300 -b google

نکته: در دستور بالا میتوانید بعد از -l که محدودیت برای بررسی صفحات است عدد دلخواه خودرا بنویسید و همچنین به جای گوگل وب سایت منبع موردنظر رو وارد کنید مثلا : bing

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
* TheHarvester Ver. 2.7                                             *
* Coded by Christian Martorella                                     *
* Edge-Security Research                                            *
* cmartorella@edge-security.com                                     *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...


[+] Emails found:
------------------
info@baseiran.com
domain@baseiran.com

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
185.55.227.88:whois.baseiran.com
185.55.227.88:www.baseiran.com
root@kali:~# 
```

مطابق تصویر صفحه قبل مشاهده کردید که دوتا ایمیلی که به دامنه متصل هستند رو پیدا کرد و به مانشان داد ، درپایین هم ساب دامین ها و DNSهای مربوط به آن را نیز برای ما نشان داد.

ما میتونیم از همین روش برای همین دامین از linkedin هم استفاده کنیم ، بنابراین دستور رو اجرا میکنیم:

```
theharvester -d baseiran.com -l 300 -b linkedin
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Linkedin..
        Searching 100 results..
        Searching 200 results..
        Searching 300 results..
Users from Linkedin:
====================
Dr.Alireza Emami
Omid Enssani
Hadi Taghizadeh
Maryam Shirinzadeh
Anoop Kumar M S
root@kali:~#
```

دراینجا کاربرانی که داخل linkedin هستند رو برای ما لیست میکنه و اسم اکانت آنها برای ما نشان داده میشود.

ابزار بعدی "goofile" می باشد ، شما اگر این ابزار رو در کالی ورژن جدید نصب ندارید پکیجش موجوده و میتوانید با استفاده از دستور apt -get install goofile پکیج رو دانلود و نصب کنید.

ابزار goofile برای جستجو Document ها و فایل های موردنظر از google استفاده می کند.

به کمک این ابزار میتوانید فایل هایی با پسوند موردنظر داخل هاست یک وب سایت رو پیدا کنید ، مثلا من میخوام داخل وب سایت baseiran.com تمام فایل های با پسوند png رو برام لیست کنه ، بنابرین دستور رو اینجوری مینویسم:

goofile -d baseiran.com -f png

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# goofile -d baseiran.com -f png

-------------------------------------
|Goofile v1.5                       |
|Coded by Thomas (G13) Richards     |
|www.g13net.com                     |
|code.google.com/p/goofile          |
-------------------------------------


Searching in baseiran.com for png
========================================

Files found:
====================

/images/branding/googleg/1x/googleg_standard_color_128dp.png
/images/nav_logo229.png
====================

root@kali:~#
```

میبینید که لیست فایل های با این پسوند و مسیر آنها در هاست رو به ما نشون داد.

دراینجا پسوند png یک مثال بود و شما می تونید تمامی پسوندهای موردنظر خودتون رو در وب سایت موردنظر جستجو و شناسایی نمایید.

پایان بخش اول

Author : Sirvan allahvisi

More Papers : https://independent.academia.edu/SirvanVisi

E-mail : SirvanVisi@yahoo.com

25 March 2017

Kurdistan , Sanandaj